UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/517,479	12/07/2004	Franciscus Lucas Antonius Johannes Kamperman	2069.057US1	6117

21186 7590 09/26/2008

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
CHAI, LONGBIT	
ART UNIT	PAPER NUMBER
2131	
MAIL DATE	DELIVERY MODE
09/26/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/517,479	KAMPERMAN ET AL.	
	Examiner	Art Unit	
	LONGBIT CHAI	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 June 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,8-11 and 13-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,8-11 and 13-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 December 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *6/30/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Currently pending claims are 1 – 6, 8 – 11 and 13 – 18.

Response to Arguments

2. Applicant's arguments with respect to instant claims have been fully considered but are moot in view of the new ground(s) of rejection necessitated by Applicant's amendment.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1 – 5, 8 – 10 and 13 – 18 are rejected under 35 U.S.C. 102(e) as being anticipated by Revital et al. (U.S. Patent 2004/0101138), which is incorporated by reference with Tsuria (U.S. Patent 6,178,242).

As per claim 1, 8 and 13, Revital teaches a method of processing a broadcast data stream that contains a stream of encrypted data and decryption information messages, data in successive segments of the stream of encrypted data being decryptable using the decryption

information from the messages (Revital: Para [0168]: ECM message matches decryption information messages that encrypts the media content data), the method comprising:

storing the stream of encrypted data, wherein the stored stream of encrypted data does not include any entitlement control messages (Revital: Page 18 / left Column / Line 1 – 7 & Figure 5: a separate ECM memory stores a plurality of ECM messages that solely contains the ECM payload excluding the media content data (see Figure 5));

storing items with decryption information for the stored stream of encrypted data independently retrievable from the stored stream of encrypted data, wherein the items with decryption information include the entitlement control messages for decrypting the stored stream of encrypted data (Revital: Para [0126] Line 6 – 9: ECM message is used to generate the key (i.e. Control Word) to decrypt the encrypted media content data);

storing synchronization information linking respective points in the stored stream of encrypted data to respective ones of the items with decryption information (Revital: Para [0127] Line 14 – 17 / Line 11 – 14: SPI (Security Parameter Index), as taught by Revital, which is used as a synchronization pointer between the stored ECM messages and the encrypted media data content, matches the recited “synchronization information”);

replaying a stored part of the stored stream of encrypted data (Revital: Para [0007], [0073] and [0078]: a play-back device);

retrieving the items with decryption information for the points in said stored part during said replaying (Revital: Para [0126] Line 6 – 9: retrieving ECM message from the stored memory to generate the key (i.e. Control Word) to decrypt the encrypted media content data); and

combining the retrieved items with decryption information with the stored part during replay at times selected under control of the synchronization information (Revital: Para [0126] Line 6 – 9, Para [0127] Line 14 – 17 / Line 11 – 14 and Para [0068] Line 10 – 17).

As per claim 2, Revital teaches during replay the stream is fed to a decoder and the decryption information is combined with the stream by feeding the decryption information to a secure device, which in response to the decryption information feeds control words to the decoder (Revital [0006] and Para [0116] Line 1 – 5: the security module retrieve the content key from the decryption information).

As per claim 3 and 9, Revital teaches storing the items with decryption information each in association with a respective time stamp value; maintaining a progressive time stamp counter during replay of the stored stream of encrypted data; and combining each particular retrieved item with the stream in response to detection that the time stamp counter reaches the time stamp value associated with the particular retrieved item (Revital: Para [0116] Line 15 – 30: a “key period” is being tracked to synchronize the correct ECM messages).

As per claim 4 and 10, Revital teaches maintaining a further progressive time counter during reception of the stream of encrypted data; sampling values from said further time counter each time when a respective one of the messages is detected during reception; storing decryption information from said message in the items with decryption information; storing the sampled value sample for each respective one of the messages as said time stamp value associated with the item that contains decryption information from said message (Revital: Para

[0116] Line 15 – 30, Para [0126] Line 6 – 9, Para [0127] Line 14 – 17 / Line 11 – 14 and Para [0068] Line 10 – 17).

As per claim 5, Revital teaches the encrypted data contains time counting information used for controlling progress of the time stamp counter (Revital: Para [0116] Line 15 – 30, Para [0126] Line 6 – 9, Para [0127] Line 14 – 17 / Line 11 – 14 and Para [0068] Line 10 – 17).

As per claim 14 and 15, Revital teaches the decryption information recording unit is operable to trigger sampling of the entitlement control messages from the received data stream upon detection of a transition in the content of the entitlement control messages in the received data stream (Revital: Para [0116] Line 15 – 30: sampling in a order of seconds between changes and buffering the previously received / sampled ECM information and previously derived content keys in case of ECM is delayed / deterred).

As per claim 16, Revital teaches the decryption information recording unit is operable to decrypt the encrypted data output from the demultiplexer, and then to re-encrypt the decrypted data with a key that is local to the conditional access apparatus, the key not having been included in any of the entitlement management messages received in the received data stream (Tsuria: Column 3 Line 1 – 8: the decrypted data is re-encrypted by a transformed ECM key (i.e. TECM key)).

As per claim 17, Revital teaches the encrypted data includes a series of segments, and wherein the decryption information recording unit is operable to sample the segments, and to provide as an output no more than one entitlement control message corresponding to each of

the segments, output entitlement control messages including at least one control word used for decryption of a corresponding segment of the series of segments (Revital: Para [0126] Line 1 – 9: Each media data content segment is associated with a ECM message which is used to generate the key (i.e. Control Word) to decrypt the associated encrypted media data content segment).

As per claim 18, Revital teaches each of the no more than one entitlement control messages are linked to the corresponding segment by a pointer stored in the encrypted data Revital: Para [0127] Line 14 – 17 / Line 11 – 14: SPI (Security Parameter Index), as taught by Revital, which is used as a synchronization pointer between the stored ECM messages and the encrypted media data content, matches the recited “synchronization information”.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 6 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Revital et al. (U.S. Patent 2004/0101138), in view of Peterka et al. (U.S. Patent 2002/0170053).

As per claim 6 and 11, Revital does not teach expressly assigning different sequence numbers to the detected messages.

Peterka teaches assigning different sequence numbers to the detected messages (Peterka : Para [0123] Line 1 – 7: each of the ECM message can be assigned a sequence number to protect replay attack).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Peterka within the system of Revital because (a) Revital teaches, in a conditional access multimedia system, tracking a key period information to associate the respective ECM message that contains the decryption information of control words during the play-back of the recorded stream (Revital: Para [0116] Line 15 – 30, Para [0126] Line 6 – 9, Para [0127] Line 14 – 17 / Line 11 – 14 and Para [0068] Line 10 – 17) and (b) Peterka teaches providing a protection method against replay attack by using a sequence number that can corresponds to a time-stamped information of a respective ECM message / EMM message in a conditional access multimedia audio / video system (Peterka : Abstract and Para [0123] Line 1 – 7).

storing information representing the sequence numbers among the encrypted data at locations where the messages to which the sequence numbers have been assigned occurred in the stream during reception; storing each sequence number in association with a respective one of the items with decryption information that contains encryption information from the message to which the sequence number is assigned; using the sequence numbers stored among the stream to retrieve and time the items associated with the sequence numbers (Peterka : Para [0123] Line 1 – 7 & Revital: Para [0116] Line 15 – 30, Para [0126] Line 6 – 9, Para [0127] Line 14 – 17 / Line 11 – 14 and Para [0068] Line 10 – 17).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LONGBIT CHAI whose telephone number is (571)272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Longbit Chai/

Longbit Chai Ph.D.
Primary Patent Examiner
Art Unit 2131
09/24/2008